ISBN 978-981-11-0008-6
Proceedings of 2016 6th International Workshop on Computer Science and Engineering (WCSE 2016)
Tokyo, Japan, 17-19 June, 2016, pp. 161-166
doi: 10.18178/wcse.2016.06.027

Context Aware Architecture Based WSN Security for Detecting Compromised Nodes in Probabilistic Voting-Based Filtering

Su Man Nam and Tae Ho Cho +

College of Information and Communication Engineering, Sungkyunkwan University, Suwon, 440-746, Republic of Korea

Abstract. Wireless sensor networks are vulnerable to various type of attacks, such as false positive and negative attacks, due to energy and hardware constraints. It enable adversaries to easily compromise the sensor nodes and variously capture keys to generate the two attacks A probabilistic voting-based filtering scheme counters these attacks, which are generated by the compromised nodes, through the verification of message authentication codes in reports. Even though this scheme can successfully detect such attacks using en-route filtering technology, it cannot detect the compromised nodes due to data fabrication. In this paper, we propose a scheme using a context aware architecture (CAA) to successfully detect compromised nodes in addition to the above attack types. To detect the compromised nodes, the CAA analyzes real world context data and security knowledge. Experimental results indicate that all of the compromised nodes can be detected with high accuracy at the cost of consuming more energy by using the proposed communication architecture.

Keywords: wireless sensor networks, network security, probabilistic voting-based filtering scheme, context aware architecture.

1. Introduction

Wireless sensor networks (WSNs) are utilized in a variety of applications using wireless communication that do not involve their administrator due to continuous autonomous operation [1]. These sensor networks consist of a large number of sensors and a base station (BS) in a sensor field [2]. Since the sensor network resides in wide areas and hostile environments, the sensor nodes are left vulnerable to capture and security compromises. In addition, they possess a stringent energy without recharging and computational constraint. Because of such characteristics, the WSN results in a reduced network lifetime resulting from serious damage due to various attacks such as false positive and negative attacks.

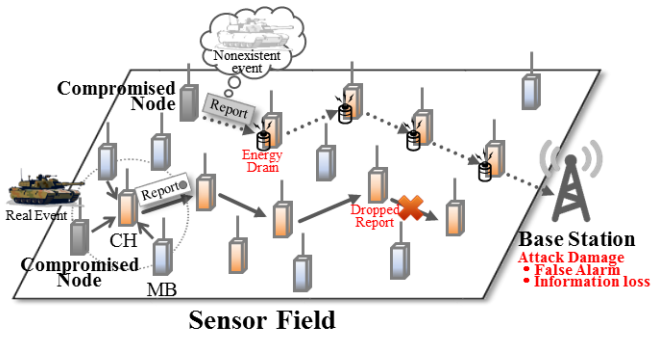

Fig. 1: False positive and negative attacks.

+ Corresponding author. Tel.: + (+82-31-290-7221).
E-mail address: thcho@skku.edu.

Fig. 1 shows false positive attacks [2, 3] and false negative attacks [2, 3] in a sensor field. For false positive attacks, a compromised node fabricates a message authentication code (MAC) [2, 3] through the absence of a real event, and its cluster head (CH) may include the false MAC in a normal report. As the report is dropped in an intermediate node, the BS loses event information. For false negative attacks, the other compromised node injects false reports into the network regarding non-existent events. The generated false report consumes unnecessary energy of its intermediate nodes and cause false alarms in the BS. These attacks result in the absence of important information and a reduced network lifetime.

A probabilistic voting-based filtering scheme (PVFS) [2] is proposed to detect both false positive and negative attacks through a predefined threshold, according to a number of false message authentication codes (MACs) in a report. In this scheme, when a false positive attack is detected, the report is continuously forwarded and when a false negative attack is detected, the report is dropped immediately. Even though this scheme effectively detects the two types of attacks at intermediate nodes, the compromised nodes persistently generate false positive and negative attacks. Context aware architecture (CAA) collects real world context data generated from the sensor network, identifies the current situation through this collected data, and provides a high level service to users. The CAA can be used as a security component of the sensor network, which can effectively prevents intrusions.

In this paper, we propose an en-route filtering scheme using a CAA to successfully detect compromised nodes in addition to the above types of attacks. To detect the compromised nodes, the CAA makes use of analysis based on real world context data and security knowledge. As a real event is generated, our proposed scheme collects context information (e.g., event data, MACs, and reports), identifies the information in the CAA, and effectively detects the compromised nodes. In this paper, the CAA is implemented based on discrete event system specification (DEVS) formalism [4]. Our proposed scheme effectively detects compromised nodes by applying CAA with only a small amount of extra energy consumption, based on real world data of the network and security knowledge of the CAA.

The rest of this paper is organized as follows. Section 2 presents the existing method and CAA. A detailed description of the proposed scheme follows in Section 3. In Section 4, a performance evaluation of the scheme is analysed. Conclusions are given in Section 5.

2. Background

In this section, PVFS and CAA are discussed in Sections 2.1 and 2.2, respectively.

2.1. PVFS

PVFS is proposed to deal with false positive and negative attacks in the sensor network. This scheme is suitable for filtering in a cluster-based model, and deploys a CH with L member nodes in a cluster. The PVFS has three phases: (1) key initialization and assignment, (2) report generation, and (3) en-route filtering. In the initialization and assignment phase, every node selects one key from a global key pool of the BS. After deploying them in the sensor field, all of CHs select verification nodes based on the distance from a source CH to the BS, and distribute verification keys to their verification nodes. In the report generation phase, a source CH randomly selects s MACs after receiving them from its members, and attaches them in a report. In the en-route filtering phase, the reports are verified in the verification nodes. If the threshold is not reached, the report is continually forwarded; if the threshold is reached, the report is dropped directly in a verification node.

2.2. CAA

The CAA automatically collects real world context data, recognizes the current status through the collected context data, and offers a high level service to users. The CAA featuring context awareness based on WSNs has preceded various related research, such as disaster countermeasures, smart homes, healthcare, etc. [5]. This CAA can be applied as a WSN security component to effectively detect intrusions [6].

3. Proposed Method

In this section, the proposed scheme is detailed.

3.1. Assumption

The sensor network is comprised of a BS, powerful nodes (e.g., H-sensors [7]), and numerous member nodes (e.g., L-sensors [7]). Every CH forwards reports to the BS along a single path. Data collection nodes (DCNs) in the communication architecture (Comm-Arch) emphasize energy to forward all of the packets from the WSN to the CAA. The CAA is implemented on a high performance computer such as the BS.

3.2. Architecture of Proposed Scheme

In the sensor network, the existing schemes effectively detect false positive and negative attacks in intermediate nodes; however, it is difficult to detect the compromised nodes which injected these attacks. In addition, if the attacks are continually generated, the sensor network will be damaged. In this paper, our proposed scheme aims to detect compromised nodes by using the CAA to ward off false positive and negative attacks. The proposed scheme mutually complements the PVFS and CAA with unified operation. In this proposal, the CAA is defined based on DEVS.

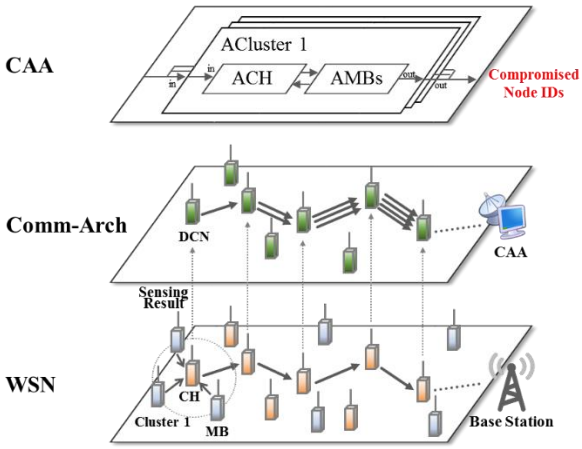

Fig. 2: Concept of the proposed scheme.

Fig. 2 presents the concept of the proposed scheme. Real world WSNs are composed of a large number of CHs and MBs with cluster-based organization. As the sensor nodes transmit packets (event data, MACs, reports, etc.), Comm-Arch collects and forwards all of the packets to CAA. The CAA models corresponding to the real world sensors perform an intelligent decision after collecting the packet data.

Our proposed scheme effectively detects all of compromised nodes by applying CAA. That is, the proposed scheme maintains the security levels of the existing scheme in addition to seeking any compromised nodes.

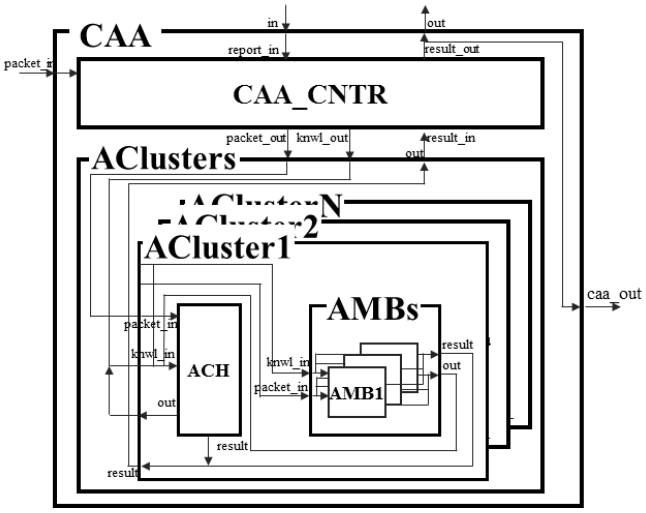

Fig. 3: DEVS models for CAA.

Fig. 3 illustrates the DEVS model for the CAA of the proposed scheme. Models in the CAA correspond to real world WSNs (BS→CAA_CNTR, Cluster→Acluster, CH→ACH, MB→AMB, etc.). The CAA has an in-port for the CAA called *packet_in*, which inputs all of the real world data through Comm-Arch, and an out-port called *caa_out*, which outputs compromised node IDs. To detect compromised nodes in CAA, it is important to analyze real world data and security knowledge in the CAA models. The core models in the CAA are ACH and AMB for detecting the compromised nodes, and the two models have same state transition.

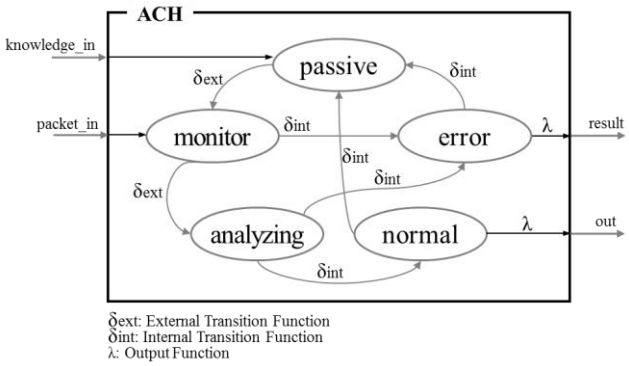

Fig. 4: State transition diagram of the ACH.

Fig. 4 presents a state transition diagram of the ACH. For example, if a false negative attack is generated in the sensor network implemented in PVFS, a compromised node injects a false report with some fabricated MAC. If the false report is continually forwarded via verification nodes, the nodes consume unnecessary energy. Even though the BS can verify the false report, it will not know the location of the compromised node because the node can fabricate a source ID of the report or can use a captured key from another node. After the CAA collects all of the real world packet data through the Comm-Arch, the ACH detects the compromised nodes based on the data and security knowledge (e.g., passive → monitor → analyzing → error).

4. Simulation Results

A simulation was performed to evaluate the proposed scheme and compare it to PVFS. The sensor field has a BS and 1,000 sensor nodes (100 CHs, 900 members), and the size of the simulation environment was 1,000 1,000 m2. The BS was located in the lower-middle of the sensor field. The initial energies of the DCN, CH, and MB were 3 J, 2 J, and 1 J. Each node employed 16.25 μJ per byte to transmit, 12.5 μJ per byte to receive, and 15 μJ per byte to generate packets. In addition, each verification node consumed 75 μJ to verify the MAC. In this simulation, 250 events were randomly generated in the sensor field. The environment was set to 10 compromised nodes for false positive and negative attacks.

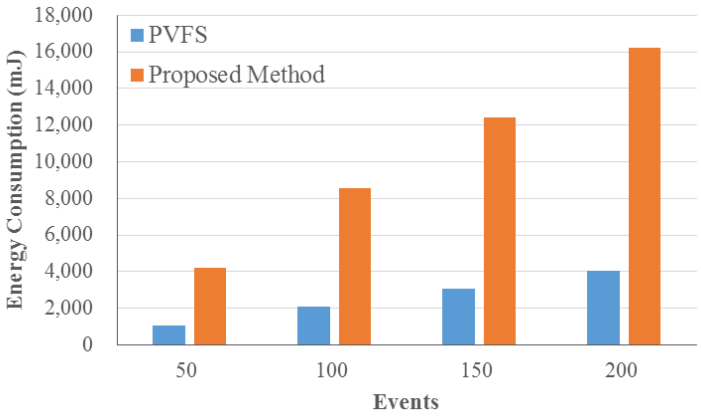

Fig. 5: Energy consumption versus the events.

In Fig. 5, the energy consumption versus the number of events is presented for the PVFS and the proposed scheme with a false traffic ratio of 10%. Even though the proposed scheme consumes about 5 J more by using Comm-Arch as compared to the existing scheme, the energy consumption difference is small compared to the energy consumed by Comm-Arch (300 J).

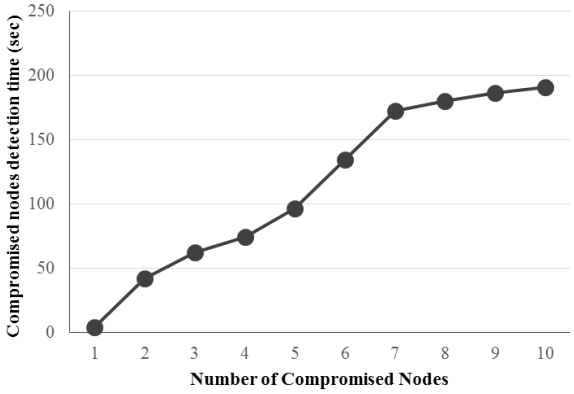

Fig. 6: Compromised node detection time versus the number of compromised nodes.

Fig. 6 shows simulation time needed to detect all of the compromised nodes. In general, the sensing time, MAC collecting time, reporting time, and verifying time are 1 ms, 4 ms, 1 ms, and 28 ms, respectively. To forward a report, about 0.4 s is spent from the largest hop to the BS. All of compromised nodes are detected within about 193 s (a report is generated per 2 s). Therefore, the time spent in the simulation for node detection is practical for the proposed scheme.

5. Conclusions

In the sensor network, sensor nodes are easily compromised and they can generate false positive and negative attacks. These attacks result in information loss and energy wastage. In addition, compromised nodes cannot be easily detected due to data fabrication. The proposed scheme effectively detects the compromised nodes and attacks by using CAA. Even though the proposed scheme consumes more energy due to the use of the Comm-Arch, the energy gap is allowed to detect all of the compromised nodes in the sensor network. In future work, we will study how the detected compromised nodes respond in various simulation environments.

6. Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2013R1A2A2A01013971)

7. References

[1] K. Akkaya, and M. Younis. A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks, Elsevier* 2005, **3** (3): 325-349.

[2] F. Li, A. Srinivasan, and J. Wu. PVFS: A probabilistic voting-based filtering scheme in wireless sensor networks. *International Journal of Security and Network* 2008, **3**: 173-182.

[3] F. Ye, H. Luo, S. Lu, and L. Zhang. Statistical en-route filtering of injected false data in sensor networks. *Selected Areas in Communications, IEEE Journal* 2005, **23**: 839-850.

[4] B. P. Zeigler. Object-oriented simulation with hierarchical, modular models: intelligent agents and endomorphic systems. *Academic press*, 2014.

[5] C. Wang, R. Hwang, and C. Ting. UbiPaPaGo: Context-aware path planning. *Expert Syst.Appl.* 2011, **38**: 4150-4161.

[6] R. Roman, J. Lopez, and S. Gritzalis. Situation awareness mechanisms for wireless sensor networks. *Communications Magazine* 2008, **46**: 102-107.

[7] D. Xiaojiang, M. Guizani, X. Yang, and C. Hsiao-Hwa. Two tier secure routing protocol for heterogeneous sensor networks. *Wireless Communications, IEEE Transactions* 2007, **6**: 3395-3401.